

#2

PCT/EP 98 / 00827

Europäisches
PatentamtEuropean
Patent OfficeOffice européen
des brevets

REC'D 27 APR 1998

WIPO PCT

Bescheinigung

Certificate

Attestation

Die angehefteten Unterla-
gen stimmen mit der
ursprünglich eingereichten
Fassung der auf dem näch-
sten Blatt bezeichneten
europäischen Patentanmel-
dung überein.

The attached documents
are exact copies of the
European patent application
described on the following
page, as originally filed.

Les documents fixés à
cette attestation sont
conformes à la version
initialement déposée de
la demande de brevet
européen spécifiée à la
page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

97103151.3

PRIORITY DOCUMENT

Der Präsident des Europäischen Patentamts:
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

A.J. Copini

DEN HAAG, DEN
THE HAGUE,
LA HAYE, LE

14/04/98

EPA/EPO/OEB Form 1014 - 02.91

BEST AVAILABLE COPY
BEST AVAILABLE COPY



Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

**Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation**

Anmeldung Nr.
Application no
Demande n° 97103151.3

Anmeldetag
Date of filing
Date de dépôt 26/02/97

Anmelder
Applicant(s)
Demandeur(s)
SIEMENS AKTIENGESELLSCHAFT
80333 München
GERMANY

Bezeichnung der Erfindung
Title of the invention
Titre de l'invention

Redundant aufgebautes elektronisches Gerät mit zertifizierten und nicht zertifizierten Kanälen

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat
State
Pays

Tag
Date
Date

Aktenzeichen
File no
Numéro de dépôt

Internationale Patentklassifikation
International Patent classification
Classification internationale des brevets

G06F11/16, G05B9/03, G05B19/05, G06F11/277

Am Anmeldetag benannte Vertragsstaaten
Contracting states designated at date of filing AT/BE/CH/DE/DK/ES/FI/FR/GB/GR/IE/IT/LU/MC/NL/PT/SE
Etats contractants désignés lors du dépôt

Bemerkungen
Remarks
Remarques

Beschreibung

Redundant aufgebautes elektronisches Gerät mit zertifizierten
5 und nicht zertifizierten Kanälen

Die vorliegende Erfindung betrifft ein zumindest zweikanalig
aufgebautes elektronisches Gerät, insbesondere eine zweikana-
lig aufgebaute programmierbare Logik, wobei diese program-
10 mierbare Logik beispielsweise die Zentraleinheit einer spei-
cherprogrammierbaren Steuerung sein kann.

Für sicherheitsrelevante Aufgaben werden elektronische Geräte
benötigt, die in hohem Maße funktionssicher sind, wobei der
15 Ausdruck „funktionssicher“ in Anlehnung an den Ausdruck
„functional safety“ des internationalen Schriftstücks Draft-
IEC 1508 gewählt wurde.

Funktionssichere elektronische Geräte zeichnen sich dadurch
20 aus, daß für sie spezielle Maßnahmen vorgesehen sind, um Feh-
ler und Ausfälle zu vermeiden, zu erkennen und zu beherr-
schen.

Eine gebräuchliche Methode zum Vermeiden, Erkennen und Be-
25 herrschen von Fehlern und Ausfällen ist die mehrkanalige,
redundante Ausführung elektronischer Geräte - in den jeweili-
gen Kanälen werden gleiche Operationen parallel ausgeführt.
Durch Vergleich der Ergebnisse bzw. Ausgangswerte wird er-
kannt, ob in einem der Kanäle ein Fehler aufgetreten ist.

30 Eine bestimmte Gruppe von Fehlern, die für die Gewährleistung
eines funktionssicheren Betriebs von besonderer Relevanz
sind, sind die sogenannten systematischen Fehler einer Bau-
gruppe, eines Bauteils oder einer Komponente eines Kanals.
35 Derartige Fehler können z.B. durch die logische Struktur,

d.h. die Verschaltung der einzelnen Komponenten und Baugruppen untereinander, oder deren physikalischen Eigenschaften, die durch den jeweils angewandten Herstellungsprozeß bedingt sind, begründet sein. Die für die vorgesehene Anwendung ausreichende Freiheit von systematischen Fehlern wird durch umfangreiche Zertifizierungsmaßnahmen nachgewiesen.

Bei der heutigen schnellen Entwicklung der Halbleitertechnologie werden die Herstellungsprozesse bereits nach kurzer Zeit gewechselt. Dies hat zur Folge, daß für die betreffenden Komponenten und Baugruppen ihre Freiheit von systematischen Fehlern immer wieder neu nachgewiesen werden muß, denn der Betrieb derartiger Komponenten und Baugruppen in einem als funktionssicher eingestuften System ist nur nach umfangreichen Zertifizierungsmaßnahmen zulässig.

Der schnelle Innovationszyklus im Bereich der Halbleiter hat zur Folge, daß diese Zertifizierung z.B. mit jeder neuen Mikroprozessorgeneration oder jeder neuen Speicherbausteingeneration neu durchgeführt werden muß, wobei die für den Zertifizierungsprozeß aufgrund der für die zu erbringenden Tests und/oder der für den Nachweis der Betriebsbewährtheit zu veranschlagenden Zeit dazu führt, daß neuartige Bauteile erst mit erheblicher Verzögerung für sicherheitsrelevante Anwendungen eingesetzt werden können.

Die Aufgabe der vorliegenden Erfindung besteht folglich darin, ein elektronisches Gerät anzugeben, mit dem es möglich ist, in sicherheitsrelevanten Systemen mit homogen redundanten Kanälen Baugruppen, Bauteile oder Komponente zu betreiben, für welche die ausreichende Freiheit von systematischen Fehlern noch nicht nachgewiesen wurde.

Die Aufgabe wird für das elektronische Gerät dadurch gelöst, daß das zumindest zweikanalig homogen redundant aufgebaute

elektronische Gerät, das insbesondere eine zweikanalig homogen redundant aufgebaute programmierbare Logik sein kann, zumindest einen zertifizierten Kanal und zumindest einen nicht zertifizierten Kanal aufweist, wobei der zertifizierte Kanal
5 ein von systematischen Fehlern ausreichend freier Kanal ist.

Als von systematischen Fehlern ausreichend freier Kanal wird in diesem Zusammenhang ein Kanal verstanden, dessen Versagenswahrscheinlichkeit über einen bestimmten Zeitraum eine
10 bestimmte, durch die jeweilige Anwendung beeinflusste Schwelle, die z.B. eine Schwelle nach dem internationalen Schriftstück Draft-IEC 1508 sein kann, nicht überschreitet.

Wenn für jeden Kanal ein abfragbares Kennzeichen, z.B. eine
15 spezielle Speicherzelle oder ein mechanischer oder elektronischer Schalter vorgesehen ist, wobei beim Abfragen des Kennzeichens für einen zertifizierten Kanal eine erste Kennung bzw. für einen nicht zertifizierten Kanal eine zweite Kennung
20 ermittelbar ist und das elektronische Gerät seinen Betrieb nur dann aufnimmt, wenn bei der Abfrage der Kennung der einzelnen Kanäle zumindest einmal die erste Kennung auftritt, so ist damit für das elektronische Gerät ein Selbsttest realisiert, der gewährleistet, daß das elektronische Gerät seinen
25 Betrieb nur dann aufnimmt, wenn sichergestellt ist, daß mindestens einer der Kanäle des mindestens zweikanalig aufgebauten elektronischen Gerätes ein von systematischen Fehlern ausreichend freier, d.h. zertifizierter Kanal ist.

Wenn die Abfrage der Kennung der einzelnen Kanäle sequentiell
30 erfolgt, ist eindeutig ermittelbar, welcher der Kanäle ein von systematischen Fehlern ausreichend freier, d.h. zertifizierter Kanal ist und welcher der Kanäle ein von systematischen Fehlern nicht ausreichend freier, d.h. nicht zertifizierter Kanal ist.

Wenn die Kennung des nicht zertifizierten Kanals beim Betrieb des elektronischen Gerätes nach einer vorgebbaren, von erkannten Fehlern freien Zeitspanne von der zweiten Kennung, die den Kanal als nicht zertifiziert charakterisiert, auf die erste Kennung, die den Kanal als zertifiziert charakterisiert, wechselbar ist, ist nach ausreichender Betriebsdauer und Bewertung des Betriebsverhaltens des bisher nicht zertifizierten Kanals dieser Kanal selbst als Referenzkanal einsetzbar, so daß mit dem elektronischen Gerät z.B. Bauteile, Komponenten oder Baugruppen der übernächsten Generation, die natürlich noch nicht zertifiziert sind, eingesetzt werden können, ohne vorher deren Fehlerfreiheit nachweisen zu müssen.

Weitere Vorteile und erfinderische Einzelheiten ergeben sich aus der nachfolgenden Beschreibung eines Ausführungsbeispiels anhand der Zeichnung und in Verbindung mit den Unteransprüchen. Im einzelnen zeigt:

FIG 1 ein Blockschaltbild einer zweikanalig homogen redundant aufgebauten Zentraleinheit einer speicherprogrammierbaren Steuerung.

Gemäß FIG 1 ist das elektronische Gerät EG eine zweikanalig homogen redundant aufgebaute Zentraleinheit einer speicherprogrammierbaren Steuerung. Homogene Redundanz bezeichnet hier die Tatsache, daß die einzelnen Kanäle symmetrisch mit zumindest funktionsgleichen Bauteilen, Komponenten oder Baugruppen aufgebaut sind.

Beim Ausführungsbeispiel gemäß FIG 1 weist der Kanal A einen Mikroprozessor P, einen Programmspeicher I und einen Datenspeicher R auf. Der Betrieb des Mikroprozessors P wird mittels einer Überwachungseinheit W, eines sogenannten Watchdogs überwacht. Der Kanal B ist homogen redundant zum Kanal A

aufgebaut, was insbesondere anhand der gleichen Komponenten P, I, R, die jeweils auch mit gleichen Bezugszeichen versehen sind, deutlich wird.

- 5 Kanal A muß aus den Komponenten P, I, R, W aufgebaut sein, für die die Freiheit von systematischen Fehlern ausreichend nachgewiesen ist, mithin die jeweiligen Komponenten, Bauteile und Baugruppen also zertifiziert sind. Damit stellt sich Kanal A insgesamt als von systematischen Fehlern ausreichend
10 freier Kanal A dar.

- In Kanal B werden eine oder mehrere Komponenten P, I, R, W in Versionen eingesetzt, die in irgendeiner Weise verändert wurden, z.B. aufgrund eines neuen oder geänderten Fertigungsprozesses, und für die die Freiheit von systematischen Fehlern
15 noch nicht ausreichend nachgewiesen ist.

- Werden in den betreffenden Bauteilen, Komponenten oder Baugruppen von Kanal B eventuell vorhandene systematische Fehler
20 wirksam, werden diese durch Ergebnisvergleich mit Kanal A, der über die Kopplung K, die zwischen den Kanälen A und B besteht, durchführbar ist, erkannt und können somit beherrscht werden.

- 25 Damit ist es möglich, ohne Verschlechterung der Sicherheitseigenschaften in einem Kanal A, B des redundanten elektronischen Gerätes EG Bauteile, Komponenten oder Baugruppen zu verwenden, deren Fehlerfreiheit noch nicht ausreichend nachgewiesen ist, die mithin noch nicht zertifiziert sind.

- 30 Mit Hilfe des Ergebnisvergleichs werden systematische Fehler, die z.B. durch die physikalischen Eigenschaften der jeweiligen elektronischen Bauteilen, Komponenten oder Baugruppen oder durch einen veränderten Fertigungs- oder Montageprozeß
35 bedingt sind, erkannt.

Das erfindungsgemäße elektronische Gerät EG erlaubt es dem Anbieter eines derartigen Gerätes unmittelbar auf die Innovationszyklen z.B. der Halbleiterindustrie zu reagieren und
5 auch in funktionssicheren Systemen stets Bauteile, Komponenten oder Baugruppen anzubieten, die dem aktuellen Stand der Entwicklung entsprechen, auch wenn für diese Bauteile deren ausreichende Freiheit von systematischen Fehlern bisher mit einer Zertifizierung noch nicht explizit nachgewiesen ist.

10

In diesem Zusammenhang muß es als besonders vorteilhaft angesehen werden, daß mit dem erfindungsgemäßen Verfahren bzw. dem erfindungsgemäßen elektronischen Gerät EG diese Zertifizierung implizit zu erreichen ist.

15

Zu diesem Zweck ist es vorgesehen, daß für jeden Kanal A, B des elektronischen Gerätes EG eine Kennung verwaltet wird, die darüber Aufschluß gibt, ob der jeweilige Kanal A, B als von systematischen Fehlern ausreichend frei angesehen werden
20 kann. Nach einer bestimmten, insbesondere vom Benutzer frei wählbaren Zeitspanne, bei der im Betrieb des elektronischen Gerätes EG im bisher nicht zertifizierten Kanal A, B kein systematischer Fehler erkannt wurde, ist diese Kennung von „nicht zertifiziert“ auf „zertifiziert“ umschaltbar, so daß
25 auch der bisher explizit nicht zertifizierte Kanal, dessen Freiheit von systematischen Fehlern im konkreten Betrieb ausreichend nachgewiesen ist, wie ein explizit zertifizierter Kanal eingesetzt werden kann.

30 Dies ermöglicht es insbesondere in einem elektronischen Gerät EG zusammen mit diesem nunmehr „online-zertifizierten Kanal“ in einem weiteren, redundanten Kanal A, B auch Bauteile, Baugruppen oder Komponenten der übernächsten Generation von Halbleiterbauelementen einzusetzen, und sodann entsprechend
35 dem oben beschriebenen Vorgang auch für diese Komponenten

nach Möglichkeit deren ausreichende Freiheit von systematischen Fehlern nachzuweisen.

5 Damit ermöglicht der Einsatz des erfindungsgemäßen elektronischen Gerätes EG bzw. die Anwendung des erfindungsgemäßen Verfahrens jederzeit die Verwendung der neuesten Bauteile, Baugruppen oder Komponenten, die ansonsten erst nach einem zeitaufwendigen Zertifizierungsprozeß für die Anwendung in sicherheitsrelevanten Systemen freigegeben werden.

Patentansprüche

1. Zumindest zweikanalig homogen redundant aufgebautes elektronisches Gerät (EG), insbesondere zweikanalig homogen
5 redundant aufgebaute programmierbare Logik, wobei das elektronische Gerät (EG) zumindest einen zertifizierten Kanal (A) und zumindest einen nicht zertifizierten Kanal (B) aufweist, wobei der zertifizierte Kanal (A) ein von systematischen Fehlern ausreichend freier Kanal ist.
10
2. Elektronisches Gerät nach Anspruch 1, d a d u r c h
g e k e n n z e i c h n e t , daß für jeden Kanal (A,
B) ein abfragbares Kennzeichen vorgesehen ist, wobei beim
15 Abfragen des Kennzeichens für einen zertifizierten Kanal (A) eine erste Kennung (T) bzw. für einen nicht zertifizierten Kanal (B) eine zweite Kennung (F) ermittelbar ist, wobei das elektronische Gerät (EG) seinen Betrieb
20 nur dann aufnimmt, wenn bei der Abfrage der Kennung der einzelnen Kanäle (A, B) zumindest einmal die erste Kennung (T) vorliegt.
3. Elektronisches Gerät nach Anspruch 2, d a d u r c h
g e k e n n z e i c h n e t , daß die Abfrage der Kennung der einzelnen Kanäle (A, B) sequentiell erfolgt.
25
4. Elektronisches Gerät nach Anspruch 2 oder 3, d a -
d u r c h g e k e n n z e i c h n e t , daß die Kennung des nicht zertifizierten Kanals (B) nach einer
vorggebbaren, von erkannten Fehlern freien Zeitspanne von
30 der zweiten Kennung (F) auf die erste Kennung (T) wechselbar ist.
5. Verfahren zum Betreiben eines zumindest zweikanalig homogen redundant aufgebauten elektronischen Gerätes (EG),
35 insbesondere einer zweikanalig homogen redundant aufge-

bauten programmierbaren Logik, wobei das elektronische Gerät (EG) zumindest einen zertifizierten Kanal (A) und zumindest einen nicht zertifizierten Kanal (B) aufweist, wobei der zertifizierte Kanal (A) ein von systematischen Fehlern ausreichend freier Kanal ist.

5
10
15
6. Verfahren nach Anspruch 5, d a d u r c h g e -
k e n n z e i c h n e t , daß für jeden Kanal (A, B)
ein abfragbares Kennzeichen vorgesehen ist, wobei beim
Abfragen des Kennzeichens für einen zertifizierten Kanal
(A) eine erste Kennung (T) bzw. für einen nicht zertifi-
zierten Kanal (B) eine zweite Kennung (F) ermittelt wird,
wobei das elektronische Gerät (EG) seinen Betrieb nur
dann aufnimmt, wenn bei der Abfrage der Kennung der ein-
zelnen Kanäle (A, B) zumindest einmal die erste Kennung
(T) auftritt.

20
7. Verfahren nach Anspruch 6, d a d u r c h g e -
k e n n z e i c h n e t , daß die Abfrage der Kennung
der einzelnen Kanäle (A, B) sequentiell erfolgt.

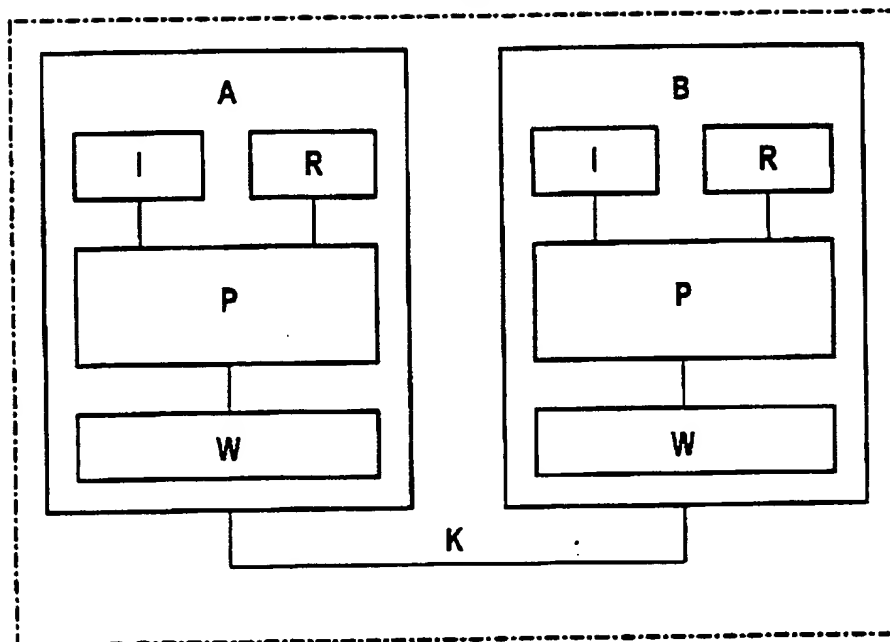
25
8. Verfahren nach Anspruch 6 oder 7, d a d u r c h
g e k e n n z e i c h n e t , daß die Kennung des
nicht zertifizierten Kanals (B) nach einer vorgebbaren,
von erkannten Fehlern freien Zeitspanne von der zweiten
Kennung (F) auf die erste Kennung (T) gewechselt wird.

51

GR 97 P 3130 E

1/1

EG



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.